UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,416	10/19/2006	Stephan J. Engberg	606-128-PCT-PA	9357

22145 7590 04/15/2008

KLEIN, O'NEILL & SINGH, LLP
43 CORPORATE PARK
SUITE 204
IRVINE, CA 92606

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/575,416	ENGBERG, STEPHAN J.	
	Examiner	Art Unit	
	CANH LE	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/18/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 01/18/2008.

Claims 1-19 have been cancelled.

Claims 20-39 have been added.

Claims 20-39 have been examined and are pending.

Response to Amendment

The applicant's amendment filed 01/18/2008 necessitated the new ground(s) of rejection presented in this Office action. Therefore, applicant's arguments with respect to claims 20-39 have been considered but are moot in view of the new ground(s) of rejection.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

There is no antecedent basis for **"a first identity device"**, **"a second identity device"**, and **"a third identity device"**, and **"a further identity device"** for claims 20, 33, 32, and 27.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 33-39 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. "means for verifying the authentication…", "means for establishing…", "means for verifying employs data…", and "means for establishing communication" critical or essential to the practice of the invention. There is no structure in the specification to support "means for plus function". See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

Claim 33 recites,

"means for verifying the authentication..." in line 6,

"means for establishing.." in line 8.

Claim 37 recites:

"means for verifying employs data…" in line 1.

Claim 39 recites:

"means for establishing communication" in line 2.

Claims **34-39** depend on claim 33 and rejected with the same reason.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 20-21, 24-25, 28-29, 33, 35, and 37 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 20 recites the limitation "the authentication" in line 6, "the identity" in line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 21 recites the limitation "the preliminary steps" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 24 recites the limitation "key" in line 6. There is insufficient antecedent basis for this limitation in the claim,

Claim 24 recites the limitation "key" in line 6 wherein its meaning is unclear. Does the key mean encrypted key and stored key?

Claim 25 recites the limitation "the group" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 28 recites the limitation "the group" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 29 recites the limitation "**dynamically**" in line 2. The term "dynamically" in claim is a relative term which renders the claim indefinite. The term "dynamically" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. See MPEP § 2173.05 (b).

Claim 33 recites the limitation "the authentication" in line 6 and "the identity" in line 11. There is insufficient antecedent basis for this limitation in the claim.

Claim 35 recites the limitation "the group" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 37 recites the limitation "the group" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-23, 26, 33-34, and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Herz** et al. (5,754,938) in view of **Andreas Pfitzmann** et al, Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology, LNCS 2009, pages 1-9, 2001.

As per claim 20:

Herz teaches a method of establishing a communication path from a first identity device in a data communication network, comprising the steps of:

(a) providing a private reference point in said data communication network **[Col. 32, lines 3-65; "our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the implementation of a set of one or more proxy servers distributed throughout the network N. .... Proxy servers may be the same or different"; a proxy server is equivalent to private reference point]**;

(b) establishing a communication path from the first identity device to said a private reference point **[Col. 31, lines 48-55, "A pseudonym is an artifact that allows a service provider to communicate with users and build and accumulate records of their preferences over time, while at the same time remaining ignorant of the users' true identities, so that users can keep their purchases or preferences private"; a user's true identity is equivalent to a first identity entity]**;

(c) verifying the authentication the first identity device relative to said a private reference point from said first identity device **[Col. 30, line 39-43; Col. 37, lines 48-53; "The proxy server may verify those credentials and make appropriate modifications to the user's profile as required by these credentials such as recording the user's new demographic status as an adult. It may also store those credentials, so that it can present them to service providers on the user's behalf"]**; and

(d) establishing communication from said a private reference point to a second identity device through said data communication network wherein at least one of the steps of verifying the authentication and establishing communication is performed without disclosing the identity of said first identity device . **[Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the bank, while still not disclosing the user's true identity to the service provider"; a second identity device is equivalent to a service provider].**

Herz is silent about one-time-use pseudonym (i.e. one-time-use reference ("privacy reference point").

However, Pfitzmann teaches one-time-use pseudonym **[pg. 6-7; Different pseudonym is used for each transaction, there is no possibility to link different transactions by equality of the pseudonyms].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the method of Herz by including the teaching of Pfitzmann because it would provide a different transaction pseudonym is used, e.g. randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by equality of pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible **[Pfitzmann, pg. 6, transaction pseudonym section].**

As per claim 21:

Herz further teaches the method according to claim 20, further comprising the preliminary steps of:

authentication said first identity device by registering data selected from the group consisting of biometrics, a signature, a code and any combinations thereof and comparing the registered data with correspondingly stored data **[Col. 31, lines 53-63; "A second and equally important requirement of a pseudonym system is that it provide for digital credentials, which are used to guarantee that the user represented by a particular pseudonym has certain properties. These credentials may be granted on the basis of result of activities and transactions conducted by means of the system for customized electronic identification of desirable objects, or on the basis of other activities and transactions conducted on the network N of the present system, on the basis of users' activities outside of network N"].**

As per claim 22:

Herz further teaches the method of claim 20, wherein the step of verifying is performed without disclosing the identity of the first identity device **[Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the**

bank, while still not disclosing the user's true identity to the service provider"; a second identity device is equivalent to a service provider].

As per claim 23:

Herz further teaches the method of claim 20, wherein the step of establishing communication is performed without disclosing the identity of the first identity device **[Col. 31, line 57 to Col. 32, line 2; "service provider may require proof that the purchaser has sufficient funds on deposit at his/her bank, which might possibly not be on a network, before agreeing to transact business with that user. The user, therefore, must provide the service provider with proof of funds (a credential) from the bank, while still not disclosing the user's true identity to the service provider"; a second identity device is equivalent to a service provider].**

As per claim 26:

Herz further teaches the method according to either of claim 20, said first identity device having an authenticated holder, and said one-time-only private reference point being addressable by the authenticated holder from a computer communicating with the data communication network **[fig. 2; Col. 30, lines 39-47; a smart cards (i.e. authenticated holder); Col. 32, lines 3-65; "our method solves the above problems by combining the pseudonym granting and credential transfer methods taught by D. Chaum and J. H. Evertse, in the paper titled "A secure and privacy-protecting protocol for transmitting personal information between organizations," with the**

implementation of a set of one or more proxy servers distributed throughout the network N. …. Proxy servers may be the same or different"].

.

Claim 33 is essentially the same as claim 20 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 34 is essentially the same as claim 21 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 38 is essentially the same as claim 22 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 39 is essentially the same as claim 23 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claims 24-25, 27-31, 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Herz** et al. (5,754,938) in view of **Andreas Pfitzmann** et al, "Anonymity,

Unobservability, and Pseudonymity - A Proposal for Terminology", LNCS 2009, pages 1-9, 2001 and further in view of **Engberg** et al. ("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6).

As per claim 24:

Herz and Pfitzmann teach the subject matter.

Herz and Pfitzmann are silent about the first identity device comprises a card including encrypted data, said method further comprising

(a) said first identity device receiving an encrypted key from said one-time-only private reference point;

(b) decrypting said encrypted key using a second stored key; and

(c) decrypting said encrypted data using said key.

However, Engberg teaches about the first identity device comprises a card including **encrypted data [pg. 1 ; abstract, user identifiers; pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"]**, said method further comprising

(a) said first identity device receiving an encrypted key from said one-time-only private reference point **[pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided**

they have the necessary computation, secure key-storage and power to do the necessary encryption etc"];

(b) decrypting said encrypted key using a second stored key **[pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"]**; and

(c) decrypting said encrypted data using said key **[pg. 1; "Using mix nets or trace-eliminating solution, devices could in theory communicate anonymously or pseudonymous provided they have the necessary computation, secure key-storage and power to do the necessary encryption etc"]**.

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 25:

Herz and Pfitzmann teach the subject matter.

Herz and Pfitzmann are silent about communication network being selected from the group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSMI network.

a code division multiplex access (CDMA) network, a universal mobile telecommunication system (UMTS) network, and any combination thereof.

However, Engberg teaches communication network being selected from the group consisting of a personal area network, local area network, a wide area network, a global area network, the Internet, a radio network, a public switched telephone network (PSTN), a global system for mobile communications (GSMI network. a code division multiplex access (CDMA) network, a universal mobile telecommunication system (UMTS) network, and any combination thereof **[pg. 1; "In ubiquitous computing macro (long-distance GSM, UMTS etc.) wireless communication is integrating with micro (local Bluetooth, infrared etc.) wireless communication as part of users general identity end environment management"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 27:

Herz and Pfitzmann teach the subject matter.

Herz and Pfitzmann are silent about first identity device allowing or blocking access to said one-time-only private reference point by a third identity device.

However, Engberg teaches the method according to either of claims 20, further comprising said first identity device allowing or blocking access to said one-time-only private reference point by a third identity device **[pg. 2, "The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 28:

Herz and Pfitzmann teach the subject matter.

Herz and Pfitzmann are silent about third identity device is a party selected from the group consisting of a third pasty and said first identity device.

However, Engberg teaches third identity device is a party selected from the group consisting of a third party and said first identity device **[pg. 2, "The outcome is a setup in which a PAD device can establish an authenticated wireless IP-session with the normal subscription telecom provider (STP) without the STP having any**

persistent device or user identifier to link one session with a PAD-device to the next and still have traceability in case the PAD-device user is involved in any criminal activity"].

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 29:

Herz and Pfitzmann teach the subject matter.

Herz and Pfitzmann are silent about a step of establishing communication involves creating and negotiating accountability path dynamically adapted to a context risk profile.

However, Engberg teaches a step of establishing communication involves creating and negotiating accountability path dynamically adapted to a context risk profile **[pg. 3, "Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be established are not discussed in this paper even though it is highly relevant. We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym. The data component is encrypted**

using multiple layers in such a way that it is not providing linkability by its existence and only through a series of steps including multiple trusted parts lead to disclosure of identity or other linking information ... Relevant for this paper is the consideration that possession of a data component providing such properties is not in itself identifying as identity is not readily accessible nor is it clearly anonymous as linkability exists. Privacy Accountability is structurally different from an Identity Escrow setup as in a PKI Certificate Authority as the unit in possession of the data component are only trusted to keep the data component in hiding until the disclosure process - for any reason – is required to initiate"].

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

As per claim 30:

Engberg further teaches the method according to claim 29, wherein said first identity device has an authenticated holder, and said second identity device establishes a procedure to identify a pasty selected from the group consisting of said first identity device and the authenticated holder of said first identity device **[pg. 3-4; "Key to Privacy Authentication is the existence of Privacy Accountability. The various properties of Privacy Accountability including how it could be...These operations**

should be controlled in a tamper-resistant environment such as a smart-card (i.e. authenticated holder) together with additional protection]

As per claim 31:

Engberg further teaches the method according to claim 30, wherein said procedure to identify a party employs identification information selected from the group consisting of at least one of biometrics, name, digital signature, and a code **[pg. 3, "We assume the existence of a data component incorporating either identifying (a signature, a verified biometrics) or otherwise linking information together with a verified link to the public key of pseudonym"].**

Claim 35 is essentially the same as claim 25 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 36 is essentially the same as claim 24 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 37 is essentially the same as claim 31 except that they set forth the claimed invention as a system rather than a method and rejected under the same reasons as applied above.

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Herz et al.** (5,754,938) in view of **Andreas Pfitzmann** et al, "Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology", LNCS 2009, pages 1-9, 2001 and further in view of **Engberg** et al. ("Privacy Authentication – persistent non-identification in Ubiquitous environments", August 18, 2002, pages 1-6) and further in view of **Busboon** (US 2006/0155993 A1) .

As per claim 32:

Herz and Pfitzmann teach the subject matter.

Herz further teaches:

(b) establishing communication from said second identity device to said service provider **[Col. 31, line 19 to Col. 32, line 65; "A service provider may require proof that the purchaser has sufficient fund on deposit at his/her bank"].**

(d) providing a further identity device corresponding to a financial institution **[Col. 32, lines 1-2; funds (a credential) from the bank].**

Herz and Pfitzmann are silent about

(i) said further identity device responding to said information by transmitting an payment accept to said identity provider,

(j) said identity provider transmitting payment accept to said service provider

(k) said service provider transmitting payment accept to said second identity device.

However, Engberg further teaches:

(i) said further identity device responding to said information by transmitting an payment accept to said identity provider **[pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"]**,

(j) said identity provider transmitting payment accept to said service provider **[pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"],** and

(k) said service provider transmitting payment accept to said second identity device **[pg. 5; "The Subscribing Telecom now know the PAU-unit has authenticated the Subscriber and can open the IP-sessions for general use. Payment can be either direct using digital cash, through a pre-paid, digital cash or post-paid solution with the PAU-unit"].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz and Pfitzmann of the invention by including the step of Engberg because it would provide pervasive privacy

as part of large holistic privacy framework aiming to remove the need for identification or device identifiers in wireless infrastructure **[pg. 2, 5th paragraph; Engberg].**

Herz, Pfitzmann, and Engberg are silent about an identity provider.

However, Busboon teaches:

providing an identity provider and a service provider **[par. [0024]; a communication between service provider and identity provide].**

establishing communication from said service provider to said identity provider **[par. [0024]; a communication between service provider and identity provide].**

Therefore, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to modify the method of Herz, Pfitzmann , and Engberg of the invention by including the step of Busboon because it would provide solutions for privacy and data protection problems **[par. [0023], Busboon].**

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le

April 6, 2008

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139